WHAT IS CLAIMED IS:

1. A method for performing data integration between two or more computer systems provided over a network, the method comprising:

extracting data from a first database associated with a first computer system of first type, the extracted data having a first file format and a first character-set format;

encrypting the data using a first security key;

storing the encrypted data in a shared volume provided in a storage system, the storage system being coupled to a plurality of computer systems;

receiving the encrypted data from the shared volume of the storage system at a second computer system of second type, the first and second computer system being of different computer systems;

converting the received data from the first file format to a second file format, the first file format being suitable for the first computer system and the second file format being suitable for the second computer system;

decrypting the received data using a second security key that is associated with the first security key; and

converting the received data from the first character-set format to a second character-set format, the first character-set format being suitable for the first computer system, the second character-set format being suitable for the second computer system.

2. The method of claim 1, wherein the first computer system is a mainframe system, and the second computer system is an open system, and the plurality of computer systems being associated with a plurality of different companies.

3. The method of claim 1, wherein the first file format is a counter key data format.

4. The method of claim 3, wherein the second file format is a fixed block architecture format.

5. The method of claim 1, wherein the first character-set format is an Extended Binary Coded Decimal Interchange Code (EBCDIC) format.

6. The method of claim 1, wherein the second character-set format is an American Standard Code for Information Interchange(ASCII) format.

7. The method of claim 1, wherein the first security key is a public key associated with the second computer system, and the second security key is a private key associated with the second computer system.

8. The method of claim 1, wherein the first security key is a private key associated with the first computer system, and the second security key is a public key associated with the first computer system.

9. The method of claim 1, wherein the first and second computer systems are coupled to the storage system via a storage area network and the storage system includes at least one disk array unit, wherein the first security key and the second security key are common keys.

10. The method of claim 1, further comprising:

storing the encrypted data in a first volume of the storage system, the first volume being associated with the first computer system,

wherein the plurality of computer systems are associated with a plurality of different companies.

11. The method of claim 10, wherein the shared volume is configured to be accessed only by computer systems of a given company, the first and second computer systems being associated with the given company.

12. The method of claim 1, wherein the step of decrypting the received data using a second security key is performed after the step of converting the received data from the first file format to a second file format, and the step of converting the received data from the first character-set format to a second character-set format is performed after the step of decrypting the received data using a second security key.

13. The method of claim 1, further comprising:

generating a digital signature of the first computer system using the extracted data;

transmitting the digital signature from the first computer system to the second computer system;

receiving the digital signature at the second computer system; and validating the received digital signature at the second computer system.

14. The method of claim 13, wherein the digital signature is transmitted from the first computer system to the second computer system via a first communication link that is different from a second communication link that is used to transfer the data from the first computer system to the second computer system.

15. A method for performing data integration between two or more computer systems provided over a network, the method comprising:

extracting data from a first database associated with a first computer system of first type, the extracted data having a first format that is suitable for the first computer system;

encrypting the data using a first security key; and

storing the encrypted data in a shared volume provided in a storage system, the storage system being coupled to a plurality of computer systems associated with a plurality of companies,

wherein the first security key is a public key of a second computer system, the second computer system configured to handle data having a second format, wherein the first format and the second format are different.

16. A method for sharing data between a plurality of computer systems sharing a storage system, the method comprising:

receiving an encrypted data from a shared volume of the storage system at a second computer system of second type, the encrypted data being data that has been extracted from a first volume of the storage system that is associated with a first computer system of first type;

converting the received data from a first format to a second format, the first format being suitable for the first computer system and the second format being suitable for the second computer system;

decrypting the received data using a second security key that is associated with a first security key that has been used to encrypt the extracted data at the first computer system; and

thereafter, loading the data to a second volume of the storage system, the second volume being associated with the second computer system.

17. The method of claim 16, further comprising:

converting the received data from a third format to a fourth format, the third format being suitable for the first computer system, the fourth format being suitable for the second computer system.

18. The method of claim 17, wherein the first format is a file format of first type, and the second format is a file format of second type.

19. The method of claim 17, wherein the third format is a character-set of first type, and the fourth format is a character-set of second type.

20. The method of claim 19, wherein the step of converting the received data from a third format to a fourth format is performed after the step of decrypting the received data using a second security key, and the step of decrypting the received data using a second security key is performed after the step of converting the received data from a first format to a second format.

21. The method of claim 16, further comprising:

receiving a digital signature of the first computer, the digital signature being associated with the received data; and

authenticating the digital signature of the first computer system.

22. The method of claim 21, wherein the digital signature is received via a local area network and the data is received via a storage area network.

23. A computer system, comprising:

an interface for coupling with a storage system; and

a computer storage medium including:

code for receiving an encrypted data from a shared volume of the storage system, the encrypted data being data extracted from a first volume of the storage system that is associated with another computer system that is different than the computer system,

code for converting the received data from a first format to a second format, the first format being suitable for the another computer system and the second format being suitable for the computer system, code for decrypting the received data using a second security key that is associated with a first security key that has been used to encrypt the extracted data at the another computer system, and

code for loading the data to a second volume of the storage system, the second volume being associated with the computer system.

24. A computer readable medium, comprising:

code for receiving an encrypted data from a shared volume of the storage system at a second computer system of second type, the encrypted data being data extracted from a first volume of the storage system that is associated with a first computer system of first type;

code for converting the received data from a first format to a second format, the first format being suitable for the first computer system and the second format being suitable for the second computer system;

code for decrypting the received data using a second security key that is associated with a first security key that has been used to encrypt the data at the first computer system; and

code for loading the data to a second volume of the storage system, the second volume being associated with the second computer system.

25. The computer readable medium of claim 24, wherein the first and second security keys are associated with a Public Key Cryptography standard or Common Key standard.